(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 138 320**
A2

(12) EUROPEAN PATENT APPLICATION

(21) Application number: **84305480.0**

(22) Date of filing: **10.08.84**

(51) Int. Cl.⁴: **H 04 L 9/02**, G 07 F 7/10

(30) Priority: **02.09.83 US 529161**

(43) Date of publication of application: **24.04.85 Bulletin 85/17**

(84) Designated Contracting States: **DE FR GB SE**

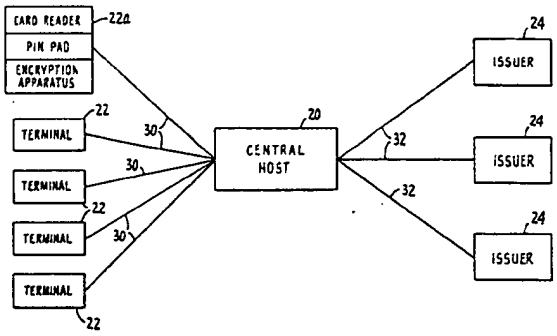
(71) Applicant: **VISA U.S.A. Inc., 101 California Street, San Francisco California 94111 (US)**

(72) Inventor: **Campbell, Carl Merritt, 809 Malin Road, Newtown Square Pennsylvania 19073 (US)**

(74) Representative: **Jackson, David Spence et al, REDDIE & GROSE 16, Theobalds Road, London, WC1X 8PL (GB)**

(54) Cryptographic key management system.

(57) A central host computer (20) is connected to a plurality of transaction card issuing institutions (e.g. banks) 24 and to a plurality of transaction terminals (22). The host (20) generates a master key which is distributed to all terminals (22), and generates a plurality of secondary keys, one for each issuer (24), each secondary key being generated by encryption of data identifying the respective issuer (24). The issuer (24) places the data identifying itself (BIN) on each card it issues. Also authorization information is encrypted under the respective secondary key and placed on the card. The authorization information can include anticounterfeiting digits or a personal identification number (PIN). When the card is applied to a transaction terminal (22), the encrypted information is read by the terminal, and also the respective secondary key is derived by the terminal (22) by encryption of the issuer identifying data (BIN) under the master key. The secondary key', thus derived is used by the terminal (22) to permit off-line analysis of the encrypted authorization information on the card by comparison with data entered manually at the terminal (22) by the card owner, and/or with non-encrypted data on the card.



EP 0 138 320 A2

Description

Cryptographic Key Management System

Technical Field

The subject invention relates to a system for distributing cryptographic keys in an electronic funds transfer (EFT) environment. The key management system is particularly suited to permit off-line verification of transaction cards at authorization terminals.

Background Art

In recent years, there has been a clear trend in society to eliminate the use of cash in financial transactions. Financial transaction cards are commonly used as a replacement for cash. These cards, which can either be credit cards or debit cards, can be used instead of cash to purchase goods or services from a merchant. Many cards can also be utilized to obtain cash or traveller's checks from financial institutions or merchants, including through the use of automatic teller machines (ATM's).

The widespread use of transaction cards has produced a concomittant increase in associated fraud. There are many types of transaction card fraud. For, example, criminals have used lost or stolen cards to purchase goods or services. Criminals have also duplicated or counterfeited cards using valid account numbers.

A number of systems have been implemented in order to reduce these fraud losses. One approach is to distribute a list of lost or stolen cards to merchants. This list must be checked at the time of purchase to see if a card, which has been presented, is valid. Unfortunately, there are difficulties with this approach. For example, it takes time to distribute the bad card list after the card has been reported lost or

stolen. Furthermore, card numbers remain on the list for only a certain period of time and when the numbers are removed, active fraud can resume. Finally, it is quite difficult to insure that all clerks in a merchant establishment will religiously refer to the card list.

Another approach, which overcomes many of the shortcomings of card lists, includes on-line authorization terminals. In this scenario, merchants are provided with electronic terminals that are connected to the issuer of the cards, possibly through a central processor. When a customer presents a card, information encoded on the card is read into the terminal. The terminal communicates this information over transmission lines to a host computer having information on the card holder. If the card is valid and the transaction does not exceed a specified limit, the host computer will return an approval to the merchant.

While this approach is an improvement over the use of bad card lists, it also has drawbacks. For example, counterfeit cards can be generated with valid account numbers which will not be screened by the system. In addition, because of high communication costs, not all transactions are typically authorized. Thus, a lost or stolen card can often be used in a remote geographical area to purchase goods.

Because of these latter shortcomings, other systems have been recently proposed to increase security. One method, which the applicant has developed, includes placing a secret, encrypted code on the card to guard against counterfeiting. Preferably, anticounterfeiting check digits are derived by encrypting the personal account number (PAN) associated with the card. These cryptographic check digits are encoded onto the magnetic stripe of the card. When the card is presented to the merchant, the information on

the magnetic stripe, which includes the PAN and the check digits, is read and transmitted to the central processor. At the central processor, the transmitted PAN is encrypted in a manner similar to the generation of the cryptographic check digits. If the two results compare favorably, the card can be authorized. As can be appreciated, without knowledge of the encryption technique used to generate the check digits, the counterfeiter merely having a valid personal account number, could not generate valid check digits.

Another approach to reducing fraud losses is to require the use of personal identification numbers (PIN's). In this technique, a particular PIN is assigned to each card holder. The PIN may be either selected by the card holder or issued by the financial institution. This approach is utilized today in many banks having automatic teller machines. When a transaction is to take place, the cardholder will enter his PIN into the terminal. The PIN is transmitted, along with the account number on the card, to the central host. The central host compares the transmitted PIN with the associated PIN stored at the central location. If these numbers match, the card holder is identified as the authorized user of the card. The latter approach is effective to reduce the unauthorized use of lost or stolen credit cards.

The above techniques, however, also have certain shortcomings. These shortcomings are becoming more severe as the geographical reach of the card systems increase. More specifically, both of the above discussed security techniques require that information be transmitted from the merchant to a remote issuer. The communication costs involved in these situations is directly related to the distance between the merchant and the card issuer. Furthermore, as the number of card holders increases, the burdens on computer time

also become significant. Therefore, it would be desirable to provide improved security system which can be utilized without having to incur communication costs. This goal can be met through the use of off-line approval techniques.

There have been some off-line approaches suggested in the prior art. One example includes the comparison of at least a portion of a cardholder's PIN, at the terminal. In this approach, a portion of the PIN is encrypted and encoded onto the magnetic stripe of the card. The key which is used to encrypt the partial PIN values is supplied to the transaction terminals. When the card is used in a transaction, the encrypted information is read from the magnetic stripe and compared with the PIN entered by the card holder, utilizing the secret key stored at the terminal. By this arrangement, a degree of security can be provided without incurring any communication costs. The partial PIN check can be used to authorize low value transactions. If a higher level transaction needs to be authorized, the remainder of the PIN can be verified through the communication network in an on-line manner. The off-line approach can also be adapted for use with the anticounterfeiting scheme outlined above.

The basic drawback to the off-line approach suggested in the prior art is that there has been no suitable method designed for distributing the encrypting keys throughout the system. Thus, while the latter system can be implemented on a small scale, difficulties arise where there are thousands of transaction terminals and hundreds of institutions issuing cards. Obviously, the simplest answer is to use a single encrypting key for all the institutions, which is then provided to all the terminals. While the keys stored in terminals can be controlled, it is difficult to provide for key security at a large number

of issuing institutions. More specifically, terminals can be safely loaded with an encrypting key during manufacture. Furthermore, these terminals can be secured to prevent tampering. However, where a large number of banks are involved, the security of the entire system would be dependent on the security of the weakest link in the group. For example, dishonest employees at one bank could conspire to uncover the key which controls the system. If the key were discovered, the entire off-line system would be compromised. Therefore, in this system, each issuing institution would be forced to rely on the security of all other issuers to guard against fraud.

To overcome the latter problem, each of the institutions could be provided with their own encrypting key. Thus, if the security at any institution were compromised, the rest of the institutions in the system could still operate. The latter approach, however, would require that each terminal be provided with the encrypting keys of each and every institution. Because of the number of institutions, this approach is deemed unfeasible as a long term solution. Therefore, it would be desirable to provide a key management system which would overcome the shortcomings described above.

Accordingly, it is an object of the subject invention to provide a new and improved key management system.

It is another object of the subject invention to provide a new and improved key management system particularly suited for off-line authorization of a transaction card.

It is a further object of the subject invention to provide a new and improved key management system particularly suited for the electronics funds transfer environment.

It is still another object of the subject invention to provide a new and improved key management system permitting the off-line verification of the authenticity of a transaction card at a terminal.

It is still a further object of the subject invention to provide a new and improved key management system which facilitates the off-line verification of the identity of a card holder utilizing a transaction card at a terminal.

Disclosure of Invention

In accordance with these and many other objects, the subject invention provides for a key management approach for use in a system which includes a plurality of issuing institutions and a plurality of transaction terminals. The system is intended to facilitate the off-line authorization of a transaction card at a terminal. In the subject system, a central host is given the responsibility of managing the keys. Typically, the issuing institutions are connected by communication lines to the host. In addition, the terminals are also connected by communication lines to the host. By this arrangement, some transactions may be authorized in a typical on-line manner utilizing the communication lines. The subject system also permits security and fraud analysis to take place in an off-line manner.

In accordance with the subject system, the central host will generate a master encryption key. The master key will be supplied to each and every terminal in the system. It is intended that the terminals be designed such that if someone tampered with the terminal, the master key would be erased or destroyed.

The central host also distributes encrypting keys to each issuing institution. These encrypting keys are derived keys. More particularly, each issuing

institution will typically have some form of identification number (i.e. Bank Identification Number, BIN). The encryption key sent to the institution is derived by encrypting the BIN, associated with the bank, under the master key. For the remainder of the specification, the term issuing institution and bank will be used interchangably. It should be understood that the scope of the subject invention includes any institution which issues financial transaction cards.

When the institution issues the card, a set of data is placed on the card. Among this data is the institution's identification number (BIN). In accordance with the subject invention, the institution will also place authorization information on the card. As discussed more fully hereinbelow, this authorization information can include anticounterfeiting data, personal identification numbers or even dynamic signature information. In any case the authorization information is placed on the card in encrypted form. Furthermore, the authorization information is encrypted under the secondary key associated with the institution.

When a card holder initiates a transaction, the information from the card is read by the terminal. In order to authorize the transaction, the secondary key must be derived by the terminal. The secondary key is derived by utilizing the master key stored in the terminal to encrypt the BIN placed on the card. Once the secondary key has been derived, it can be used to permit the analysis of the encrypted authorization information placed on the card.

The methods for analyzing the encrypted information on the card will vary depending on the particular authorization technique implemented. A number of comparison schemes are set forth in the detailed description. It is intended that the scope of

the subject invention cover any of these comparisons schemes.

The above approqach solves the shortcomings found in the prior art. More specifically, it permits off-line authorization of transaction cards at a terminal. Furthermore, since each individual issuing institution is provided with unique encrypting keys, the compromise of any single issuer's secondary key will not affect the security of the entire system. From a commercial standpoint, it is necessary to have each individual institution responsible for its own security. This result is achieved with the key management approach of the subject invention. In addition, while each individual bank is given its own unique key, there is no requirement for each terminal to be provided with all of the keys. Rather, the terminal derives the necessary secondary key utilizing the master key supplied by the central host and the bank identification number. Thus, the terminal does not require large storage capacity but only needs to be provided with one secure master key.

Further objects and advantages of the subject invention will become apparent from the following detailed description taken in conjunction with the drawings in which:

Brief Description of Drawings

Figure 1 is a diagram of a typical electronic funds transfer system in an intercharge network.

Figure 2 is a composite flow chart illustrating the steps to implement the general concept of the key management system of the subject invention.

Figure 3 is a composite flow chart illustrating the steps necessary to implement a key management system for use with an anticounterfeiting technique.

Figure 4 is a composite flow chart, similar to Figure 3, including another embodiment of an anticounterfeiting technique.

Figure 5 is a composite flow chart illustrating the key management system of the subject invention for use with the distribution of personal identification numbers (PIN's).

Figure 6 is a composite flow chart of the key management system of the subject invention showing another embodiment for use in conjunction with the distribution of PIN's.

Best Mode For Carrying Out The Invention

Referring to Figure 1, there is shown a typical configuration for an electronics funds transfer system. More specifically, a central host 20 is shown which acts as a network switch, routing information between a plurality of transaction terminals 22 and issuing institutions 24. The issuing institutions can be banks or other service organizations which distribute transaction cards, such as credit cards or debit cards. These cards may be used at various merchants or institutions to purchase goods or services or to obtain cash.

Each merchant is provided with one or more terminals 22. As shown at 22A, a terminal typically includes a reader for receiving information encoded on the magnetic stripe of the card. In addition, the terminal may include a PIN pad to permit a customer to enter their personal identification number (PIN). In accordance with the subject invention, the terminal will also include an encryption apparatus which may be provided in the main portion of the terminal or separately in the PIN pad. The location of the encryption apparatus will depend on the particular technique being selected.

Each of the terminals is connected to the host along communication lines 30. The host is also connected to the issuers along communications lines 32. In many transactions, information about the card holder and the purchase are transmitted from the terminal, along communication lines 30, to the host. Frequently, the central host will make the approval or denial decision. In other cases, the information is routed along lines 32, to the institution which issued the card. The authorization decision made by the institution is retransmitted to the merchant along the same communication lines.

As can be appreciated, as the use of bank cards increases in scope and geographical area, these communication costs will escalate. Therefore, it is desirable to provide some form of security through off-line analysis. In the subject specification, the term off-line is defined to mean operations which can be performed at the terminal without any communication to the host. These objectives are achieved with the key management system of the subject invention.

Referring now to Figure 2, the general key management system of the subject invention is illustrated. This approach can be utilized to provide both an off-line anticounterfeit check and PIN verification. The flow chart is broken into three segments where Figure 2A shows the operations performed at the central host, Figure 2B shows the operations performed by the issuer and Figure 2C shows the actions taken at the terminal.

Referring to Figure 2A, the central host or control 20 initially generates a system master key 40. This master key is supplied to all of the terminals 42. Since the security of the master key is of utmost importance, this distribution should be handled in a highly secure manner. There have been a number of

approaches designed in the prior art for distributing keys to terminals in a secure manner. In one approach, the terminals are physically connected to the host permitting initial loading of the master key. After this time, the terminals are kept under high security until they are installed at merchant locations. In another approach, a key loading device is connected to the host and has the master key loaded therein. The key loading device is then brought to each terminal and physically connected to load the key. In either approach, the terminal should be designed such that any tampering will erase or otherwise destroy the master key, such that it can never be extracted from the terminal.

The host then generates a plurality of secondary keys 44. These secondary keys are derived utilizing the bank identification number (BIN). As pointed out above, each institution is generally associated with an unique identification number. This identification number is encrypted using the master key. The resulting secondary keys are then distributed to the associated issuers. Again, a number of methods can be used to distribute the keys. Typically, secure encrypted communication lines are already established between the issuers and the host and therefore it is possible to transmit these keys over communication lines. The key may also be physically delivered using a key loading device as discussed above.

Referring to Figure 2B, the issuer is now capable of generating transaction cards. Initially, the issuer will place its BIN number on each card 50. Typically, this information is placed on the card by encoding the information on a magnetic stripe. While this approach is fairly common, there many other ways of encoding data on the cards, all of which are within the scope of the subject invention.

The issuer will then generate authorizaton information 52. As discussed below, this authorization information can be anticounterfeiting digits, PIN information or any other suitable identifier. The authorization information is then encrypted, using the secondary key supplied by the host 54. The encrypted authorization information is then placed on the card 56 in the manner described above.

The card can now be authorized in an off-line manner at the terminals. Referring to Figure 2C, the card is initially read by the terminal at 60. The terminal will typically have a card reader capable of deciphering the encoded information on the magnetic stripe. As can be appreciated, if the information is placed on the card in another manner, the terminal should have compatible reading equipment. The information which is read includes the BIN number of the institution, as well as the encrypted authorization information.

In accordance with the subject invention, the terminal will then derive the secondary key, utilizing the master key stored at the terminal to encrypt the BIN number of the institution 62. Once the secondary key has been derived, it can be used to analyze encrypted authorization information on the card 64.

Since the encrypted information had been originally encrypted under the secondary key, the analysis can be handled in a number of ways. The particular approach will depend on the system design and a few examples will be discussed in detail hereinbelow. When the information is compared, if similarity is detected, the transaction can be authorized. If the information does not match, the transaction can be denied.

Referring now to Figure 3, a more specific approach is shown for use in an anticounterfeiting

scheme. Figure 3A illustrates the actions taken at the issuer, while Figure 3B describes the events at the terminal. In Figures 3 through 6, the activities of the central host are identical with those described in Figure 2 and will not be further discussed.

In applicant's anticounterfeiting technique, the issuer will again place the BIN number on the card 70. The issuer will also generate a personal account number (PAN) which is unique for each card. This account number or (PAN) is placed on the card 72. The issuer will then encrypt the PAN with the secondary key 74. The result of this encryption is placed on the card 76. While the above discussion is limited to the use of a PAN, this number may be combined with any other information normally on the card, such as the card expiration date. Further, the entire encrypted information need not be placed on the card but only a subset thereof. By choosing only a specific subset, the information which must fit on the card can be economized.

Referring to Figure 3B, the card will be read at the terminal 80. Thus, both the BIN number and the encrypted PAN information will be received. The terminal will then derive the secondary key, utilizing the master key to encrypt the BIN 82. The secondary key is then used to encrypt the account number placed on the card at 84. The result of this encryption (or at least a portion thereof) can then be compared with the encrypted account information on the card. If these match, the transaction can be authorized.

Referring now to Figure 4, a more sophisticated anticounterfeiting approach is shown. More specifically, in the prior art, there have been developed various secure card properties. One such property is a Watermark, manufactured by Malco Plastics. Similar in concept to water marks found on paper currency, an

electronic signature can be deeply embedded in the magnetic stripe of a card. This hidden number is very difficult for counterfeiters to reproduce. Other techniques include the precise measurement of certain physical card characteristics. These technologies can be combined with the subject system to provide even further enhancement to the card.

Referring specifically to Figure 4A, the issuer will again place the BIN on the card 90. The PAN is also placed on the card 92. In addition, the secure card property, such as the Watermark is placed on the card. Because of the manufacturing sophistication necessary to implant a secure property, this step will typically be initially handled by an entity other than the issuer. The cards with the secured property placed thereon will then be supplied to the issuer. Thus, it is not intended that the order of the placement of the information on the card restrict the scope of the subject invention. The secure property, which would provide some form of numeric information, is then combined with the account number and encrypted, using a secondary key 96. The result of this encryption is then encoded on the card 98.

Referring to Figure 4B, the information on the card, including the secure property, is read by the terminal 100. The secondary key is derived, utilizing the master key to encrypt the BIN 102. The PAN and secure property are combined and are encrypted using the secondary key 104. The result of this encryption is then compared with the encrypted information encoded on the card 106. As in the previous cases, if the information matches, the transaction can be approved. However, if the information does not match, the transaction can be denied.

Referring now to Figure 5, the use of the key management system is illustrated for use with

information particularly associated with the card holder, such as a PIN. The identical system can be used for any other information associated with a specific card holder, such as dynamic signature analysis information. In the latter case, the handwriting analysis information, unique to the cardholder, would be encoded in numeric form and encrypted, using the proper key. For simplicity, the remainder of discussion of Figures 5 and 6 will be restricted to the use of PIN's.

Referring specifically to Figure 5A, the issuer will once again place its BIN number on the card 110. A PIN will then be generated to be associated with the customer. Frequently, the bank generates this PIN. The PIN may also be supplied to the issuer by the cardholder. The particular approach taken can be left to the discretion of the issuing institution as there are various advantages and disadvantages with both techniques. The benefits of each technique is discussed in detail in a bulletin by the American National Standards Committee (ANSI) publication on Pin Management and Security, ANSI-X9.8 (1982). If the PIN has been generated by the institution, it must be supplied to the cardholder.

The PIN which has been selected is then encrypted using the secondary key 114. The result of this encryption is then placed on the card 116. As pointed out above, this system is probably best utilized using only a partial PIN value. For example, where four digits constitute the PIN, only two digits are encrypted and placed on the card. The remaining two digits are utilized for higher value, on-line authorization. The partial PIN digits may also be derived using the full PIN. All or only a portion of these derived digits may be placed on the card. The

details of implementing a partial PIN system are known in the prior art and need not be discussed in detail.

Referring to Figure 5B, the card to be used is read by the terminal 120. As in all cases, the secondary key is derived by encrypting the BIN utilizing the master key stored at the terminal 122. The card holder will then enter his PIN. The PIN may be entered through the PIN pad of the terminal 124. The secondary key is then utilized to compare the encrypted PIN information on the card with the PIN entered by the card holder 126. This comparison may be carried out either by encrypting the PIN entered by the card holder or by decrypting the encrypted PIN on the card such that both PINs are in clear text.

The approach laid out in Figure 5 may be used to handle PIN information. Most encryption systems being implemented today utilize the Data encryption standard (DES), approved by the National Bureau of Standards. In this system, 64 bits of information are encrypted to generate 64 bits of enciphered output. If any of these bits are removed, decryption cannot take place. Because of the storage capacity of the magnetic stripe on a transaction card, it is often desirable to minimize the amount of information which needs to be encoded. A variety of techniques have been developed to achieve this result. One of the approaches is known generally as PIN offset generation. The latter approach is indicated in Figure 6 and requires less information to be encoded on the card.

Referring specifically to Figure 6A, the issuer places the BIN number on the card 130. In addition, the PAN is placed on the card 132. A PIN is generated 134 in a manner described above. In this embodiment, rather than encrypting the PIN, the PAN is encrypted 136. The resulting encryption is then combined with the PIN to define a coded value 138. There are a

number of ways to combine the encrypted PAN with the PIN. In the preferred embodiment, a portion of the encrypted PAN is added to the PIN using a modulo 10 procedure. Other more sophisticated approaches may be taken. In any case, the coded value is then placed on the card 140.

Referring to Figure 6B, at the initiation of the transaction, the card is read at the terminal 150. The PIN is received from the cardholder 152. The secondary key is then derived utilizing the master key to encrypt the BIN 154. The PAN is then encrypted under the secondary key 156. The encrypted PAN is then compared with the information placed on the card. This can conveniently be done in two ways, as shown at 158 and 160. More specifically, the encrypted PAN (or a portion thereof) is combined with the coded value and then compared with the PIN entered by the card holder. Where the original combination at 138 was by addition, the encrypted PAN is subtracted from the coded value, which should yield the PIN. Another alternative (160) is to combine the newly encrypted PAN (or a portion thereof) with the PIN entered by the card holder. This result should generate the coded value which has been placed on the card. In either case, if the comparison matches, the transaction can be authorized.

In summary, there has been provided a new and improved key management system, for use in an EFT environment, which permits off-line authorization of a transaction card. In the subject system, a central host generates a master key which is then supplied to all the terminals in the system. The host then derives a secondary key for each issuing institution by encrypting the BIN number of the issuing institution under the master key. The secondary keys are then supplied to the issuing institution.

When the institution issues a card, it places its BIN number on the card. In addition, authorization information is placed on the card in encrypted form. This information is encrypted under the secondary key associated with the institution. This information may include anticounterfeiting digits or PIN information. At the terminal, the information on the card is read. The terminal then derives the secondary key, utilizing the master key stored at the terminal to encrypt the BIN of the institution. The secondary key is then used to permit analysis of the encrypted authorization information which has been placed on the card. By this arrangement, off-line authorization can be carried out to enhance the security of the transaction card network. Furthermore, each of the issuing institutions is given a different cryptographic key, thereby further enhancing overall system security.

The disclosure has included a description of a number of different security approaches which can utilize the subject key management system. These techniques can be used alone or in combination. If used in combination, it could be beneficial to have the issuing institutions use a different secondary key for each technique. This could be accomplished in a number of ways. For example, a different master key could be generated for each technique, or the BIN could be modified in a set way before it is encrypted.

While the subject invention has been described with reference to a preferred embodiment, it should be understood that various other changes and modifications could be made therein, by one skilled in the art, without varying from the scope and spirit of the subject invention as defined by the appended claims.

Claims:

1. A method of distributing cryptographic keys in a system having a plurality of issuing institutions and a plurality of transaction terminals, said method comprising the steps of:

generating a master key;

supplying the master key to each terminal;

deriving a secondary key for each issuing institution by encrypting data identifying the issuing institution under the master key;

supplying the secondary keys to the associated issuing institutions;

placing said data identifying the issuing institution on said card; and

placing authorization information on each said card, said authorization information having been encrypted in the secondary key associated with the institution issuing the card, whereby a card can be authorized at any terminal by deriving said secondary key utilizing the master key stored at the terminal to encrypt said information identifying said issuing institution placed on said card thereby permitting analysis of said encrypted authorization information placed on said card.

2. A method of distributing cryptographic keys in a system having a plurality of issuing institutions and a plurality of transaction terminals, said method to facilitate the off-line verification of the authenticity of a financial transaction card at a terminal, said method comprising the steps of:

generating a master key;

supplying the master key to each terminal;

deriving a secondary key for each issuing institution by encrypting data identifying the issuing institution under the master key;

supplying the secondary keys to the associated issuing institutions;

placing said data identifying the issuing institution on said card;

generating unique account information for each card;

placing said account information on the associated card;

deriving authorization information for each card by encrypting the associated account information under said secondary key; and

placing at least a portion of said encrypted authorization information on said card, whereby the authenticity of the card can be verified by deriving said secondary key utilizing the master key stored at the terminal to encrypt said information identifying said issuing institution placed on said card and thereafter utilizing said secondary key to permit the comparison of the encrypted authorization information and the account information placed on said card.

3. A method of distributing crytographic keys as recited in claim 2 wherein said comparison is carried out by utilizing the secondary key derived at the terminal to encrypt the account information placed on the card and comparing the encrypted result to the encrypted authorization information placed on the card.

4. A method of distributing cryptographic keys as recited in claim 2 further including the step of placing a secure card property on the card, and wherein the step of deriving authorization information includes encrypting the secure card property in combination with the account information.

5. A method of distributing cryptographic keys in a system having a plurality of issuing institutions and a plurality of transaction terminals, said method to facilitate the off-line verification of the identity of a card holder utilizing a financial transaction card at a terminal, said method comprising the steps of:

generating a master key;

supplying the master key to each terminal;

deriving a secondary key for each issuing institution by encrypting data identifying the issuing institution under the master key;

supplying the secondary keys to the associated issuing institution;

placing said data identifying the issuing institution on said card;

generating personal identification information for each card and associated with each card holder;

encrypting the personal identification information under the secondary key associated with the institution issuing the card; and

placing at least a portion of the encrypted personal identification information on each said card, whereby the identity of the card holder may be verified by deriving said secondary key utilizing the master key stored at the terminal to encrypt said information identifying said issuing institution placed on said card and thereafter utilizing the secondary key to permit the comparison of the encrypted personal identification information on the card with the personal identification information entered into said terminal by said card holder.

6. A method of distributing cryptographic keys as recited in claim 5 wherein said comparison step is carried out by utilizing the secondary key derived at the terminal to decrypt the personal identification information placed on the card and comparing the result to the personal identification information entered into the terminal by the card holder.

7. A method of distributing cryptographic keys as recited in claim 5 wherein said comparison step is carried out by utilizing the secondary key derived at the terminal to encrypt the personal identification information entered into the terminal by the card holder and comparing the result to the encrypted personal identification information placed on the card.

8. A method of distributing cryptographic keys in a system having a plurality of issuing institutions and a plurality of transaction terminals, said method to facilitate the off-line verification of the identity of a card holder utilizing a financial transaction card at a terminal, said method comprising the steps of:

generating a master key;

supplying the master key to each terminal;

deriving a secondary key for each issuing institution by encrypting data identifying the issuing institution under the master key;

supplying the secondary keys to the associated issuing institution;

placing the data identifying the issuing institution on the card;

generating unique account information for each card;

placing said account information on the associated card;

generating personal identification information for each card and associated with each card holder;

encrypting the account information associated with the card under the secondary key associated with the institution issuing the card;

combining at least a portion of said encrypted account information and said personal identification information to generate a coded message; and

placing at least a portion of the coded message on the card, whereby the identity of the card holder may be verified by deriving the secondary key utilizing the master key stored at the terminal to encrypt said information identifying said issuing institution placed on said card and thereafter utilizing the secondary

key to permit the comparison of the coded message on the card and the personal identification information entered into the terminal by the card holder.

9. A method of distributing cryptographic keys as recited in claim 8 wherein said comparison step is carried out utilizing the secondary key derived at the terminal to encrypt the account information placed on the card and combining at least a portion of the result with the coded message placed on the card to permit comparison with the personal identification information entered into the terminal by the card holder.

10. A method of distributing cryptographic keys as recited in claim 8 wherein said comparison step is carried out by utilizing the secondary key derived at the terminal to encrypt the account information placed on the card and combining at least a portion of the result with the personal identification information entered into the terminal by the card holder to permit comparison with the coded message placed on the card.

11. A system for distributing cryptographic keys which include a plurality of issuing institutions and a plurality of transaction terminals, said system to facilitate the off-line authorization of a financial transaction card at a terminal, said system comprising:

control means for generating and supplying a master key to each of the terminals, said control means also for deriving a secondary key for each issuing institution by encrypting data identifying the issuing institution under the master key;

means for transmitting the secondary keys to the associated issuing institution;

means at the issuing institution for issuing cards, said means capable of placing said data identifying the issuing institution on said card, said means also for generating authorization information and encrypting said authorization information in the secondary key supplied by the central means and placing said encrypted authorization information on said card;

means at each terminal for reading said data identifying said issuing institution and said encrypted authorization information placed on the card; and

means at said terminal to derive said secondary key utilizing the master key stored at the terminal to encrypt said data identifying the issuing institution to permit analysis of said authorization information placed on said card.

12. A system for distributing cryptographic keys which includes a plurality of issuing institutions and a plurality of transaction terminals, said system to facilitate the off-line verification of the authenticity of a financial transaction card at a terminal, said system comprising:

control means for generating and supplying a master key to each of the terminals, said control means also for deriving a secondary key for each issuing institution by encrypting data identifying the issuing institution under the master key;

means for transmitting the secondary keys to the associated issuing institution;

means at the issuing institution for issuing cards, said means capable of placing said data identifying the issuing institution on said card, said means for generating unique account information for each card and placing said account information on the associated card and means for encrypting the account information under the secondary key and placing at least a portion of the encrypted authorization information on the card;

means at said terminal for reading said data identifying said issuing institution, said account information and said encrypted authorization information placed on the card; and

means at said terminal for deriving said secondary key by utilizing the master key stored at the terminal to encrypt said data identifying the issuing institution whereby the secondary key may be utilized to permit the comparison of the account information and the encrypted authorization information placed on the card.

13. A system for distributing cryptographic keys as recited in claim 12 wherein the encrypting means at said terminal utilizes the secondary key derived at the terminal to encrypt the account information placed on the card and compares at least a portion of the encrypted result to the encrypted authorization information placed on the card.

14. A system for distributing cryptographic keys as recited in claim 12 further including a means for placing a secure card property on the card and wherein the encrypting means at the issuing institution encrypts a combination of both the secure card property and the account information and places at least a portion of the result on the card and wherein the terminal includes a means for reading the secure card property.

15. A system for distributing encrypting keys which includes a plurality of issuing institutions and a plurality of transaction terminals, said system to facilitate the off-line verification of the identity of a card holder utilizing a financial transaction card at a terminal, said system comprising:

control means for generating and supplying a master key to each of the terminals, said control means also for deriving a secondary key for each issuing institution by encrypting data identifying the issuing institution under the master key;

means for transmitting the secondary keys to the associated issuing institution;

means at the issuing institution for issuing cards, said means capable of placing said data identifying the issuing institution on said card, said means capable of generating unique account information associated with said card and for placing that account information on that card, said means for generating personal identification information for each said card associated with each cardholder, said means for encrypting the account information under said secondary key and combining at least a portion of said encrypted account information with said personal identification information to generate a coded message, and thereafter placing the coded message on the card;

means at each terminal for reading said data identifying the issuing institution, said account information and said coded message placed on the card;

means at said terminal for receiving personal identification information entered by the cardholder; and

means at said terminal for deriving said secondary key utilizing the master key stored at the terminal to encrypt the information identifying said issuing institution placed on said card whereby the secondary key may be utilized to permit the comparison of the coded message on the card and the personal identification entered into the terminal by the cardholder.

16. A system for distributing encrypting keys as recited in claim 15 wherein the encrypting means at the terminal utilizes the secondary key derived at the terminal to encrypt the account information placed on the card and combines at least a portion of the result with the coded message placed on the card to permit comparison with the personal identification information entered into the terminal by the card holder.

17. A system for distributing encrypting keys as recited in claim 15 wherein the encrypting means at the terminal utilizes the secondary key derived at the terminal to encrypt the account information placed on the card and combines at least a portion of the result with the personal identification information entered into the terminal by the card holder to permit comparison with the coded message on the card.

0138320

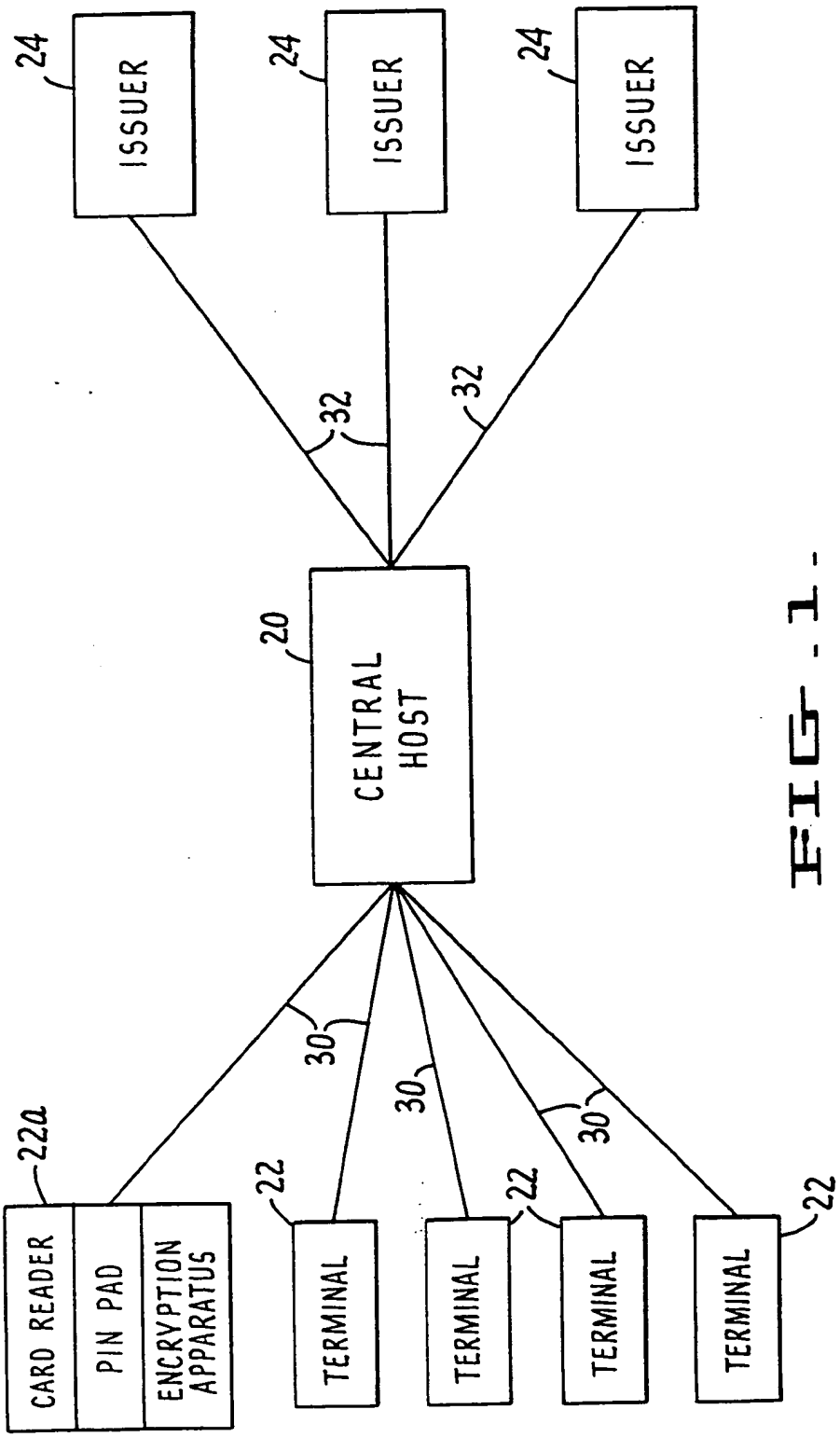


FIG. 1.

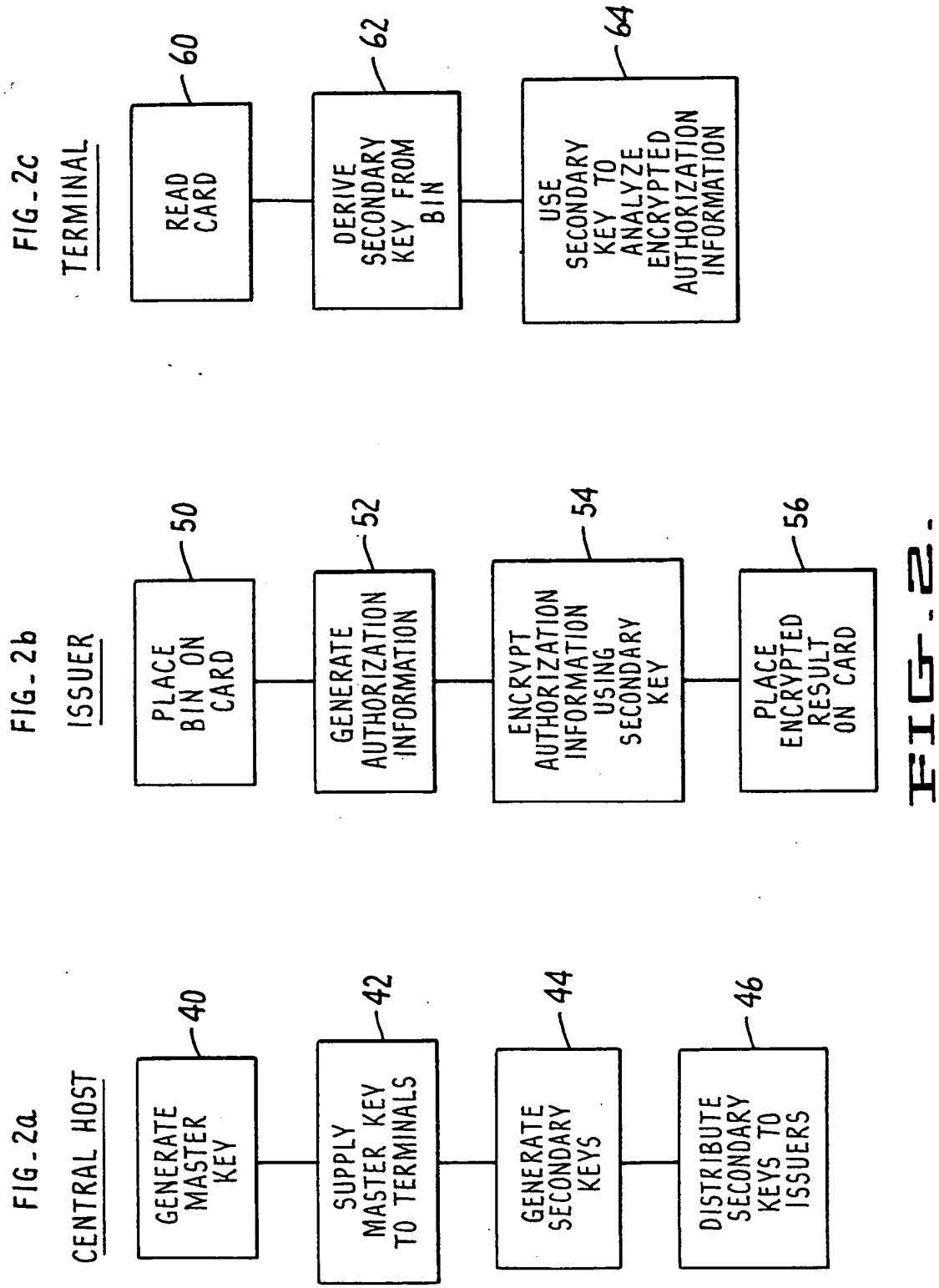


FIG-2a
CENTRAL HOST
GENERATE MASTER KEY
40
SUPPLY MASTER KEY TO TERMINALS
42
GENERATE SECONDARY KEYS
44
DISTRIBUTE SECONDARY KEYS TO ISSUERS
46
FIG-2b
ISSUER
PLACE BIN ON CARD
50
GENERATE AUTHORIZATION INFORMATION
52
ENCRYPT AUTHORIZATION INFORMATION USING SECONDARY KEY
54
PLACE ENCRYPTED RESULT ON CARD
56
FIG-2c
TERMINAL
READ CARD
60
DERIVE SECONDARY KEY FROM BIN
62
USE SECONDARY KEY TO ANALYZE ENCRYPTED AUTHORIZATION INFORMATION
64

FIG-2.

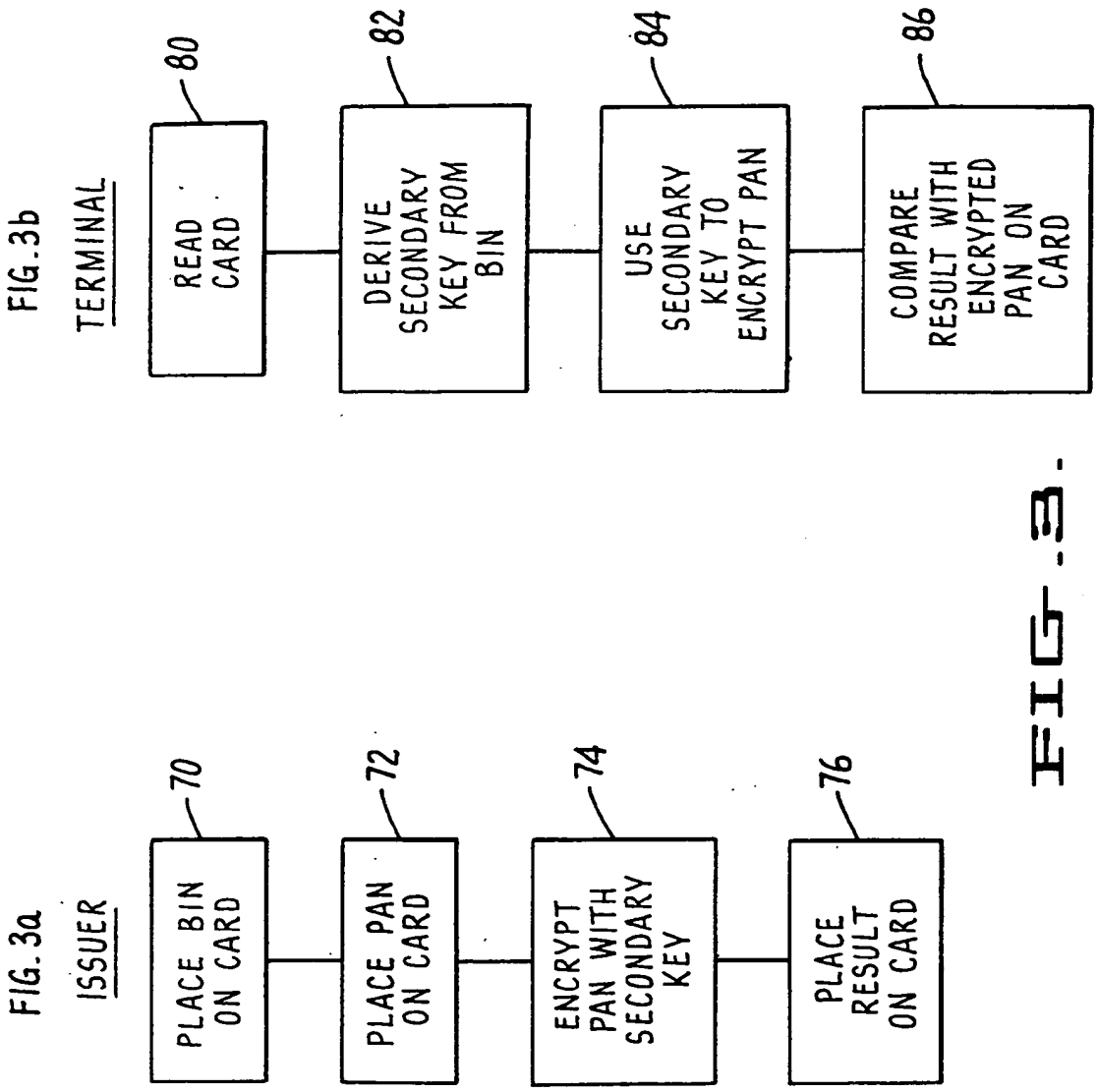


FIG. 3.

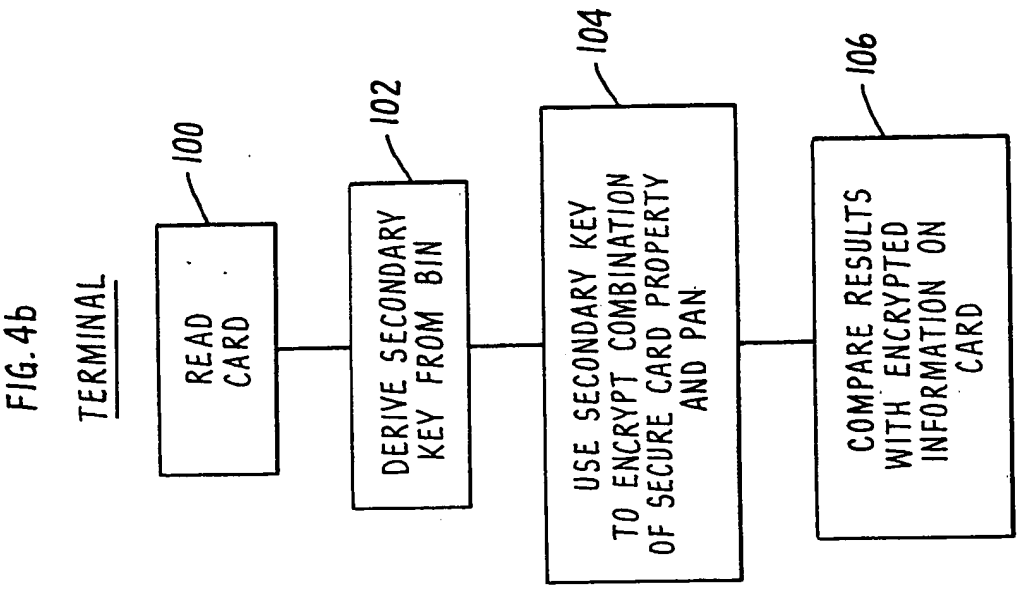


FIG.4b
TERMINAL
READ CARD
100
DERIVE SECONDARY KEY FROM BIN
102
USE SECONDARY KEY TO ENCRYPT COMBINATION OF SECURE CARD PROPERTY AND PAN
104
COMPARE RESULTS WITH ENCRYPTED INFORMATION ON CARD
106

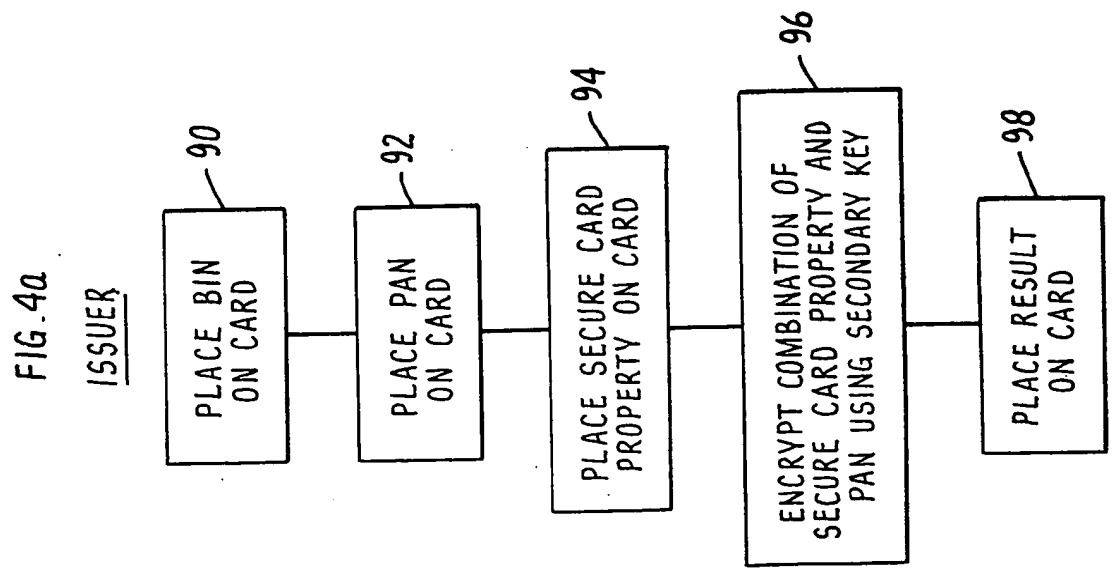


FIG.4a
ISSUER
PLACE BIN ON CARD
90
PLACE PAN ON CARD
92
PLACE SECURE CARD PROPERTY ON CARD
94
ENCRYPT COMBINATION OF SECURE CARD PROPERTY AND PAN USING SECONDARY KEY
96
PLACE RESULT ON CARD
98

FIG. 4.

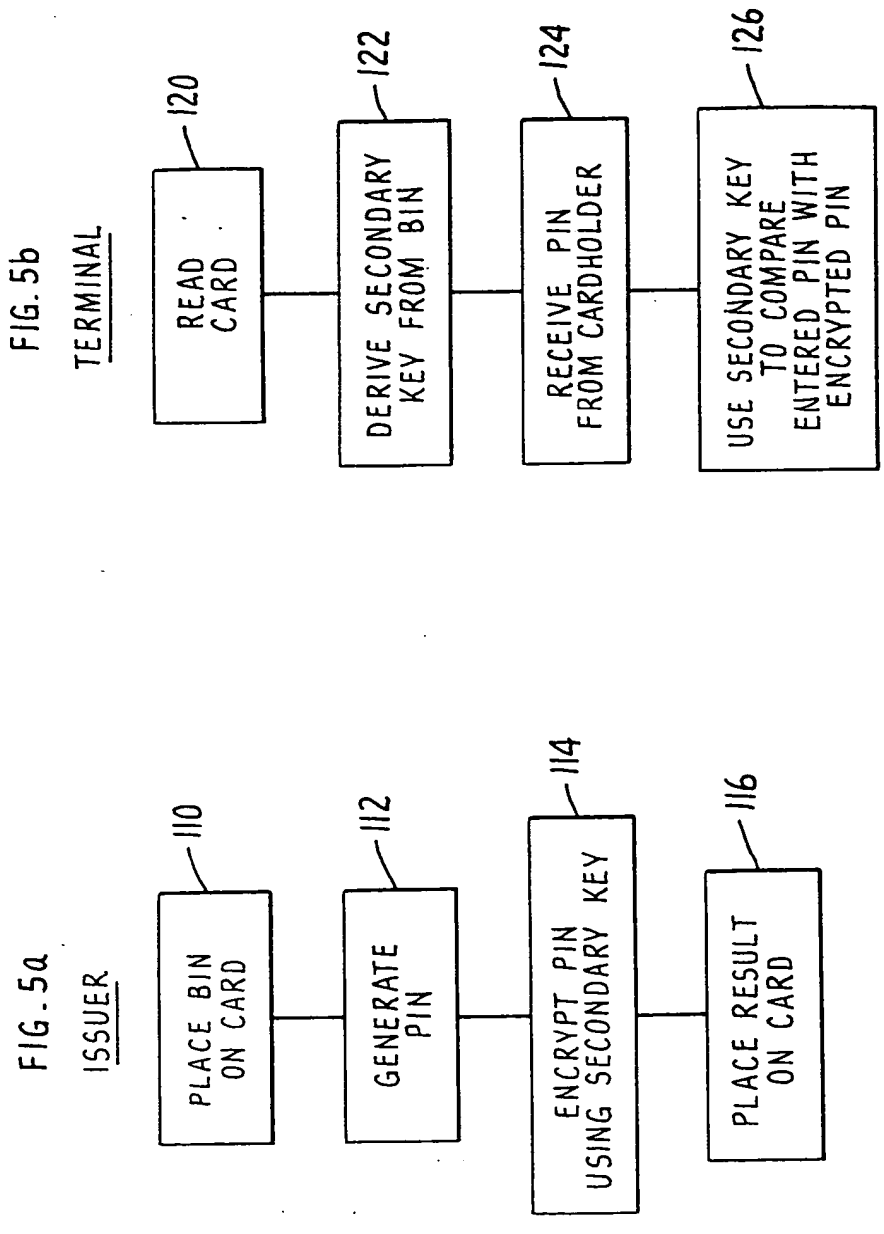


FIG. 5.

0138320

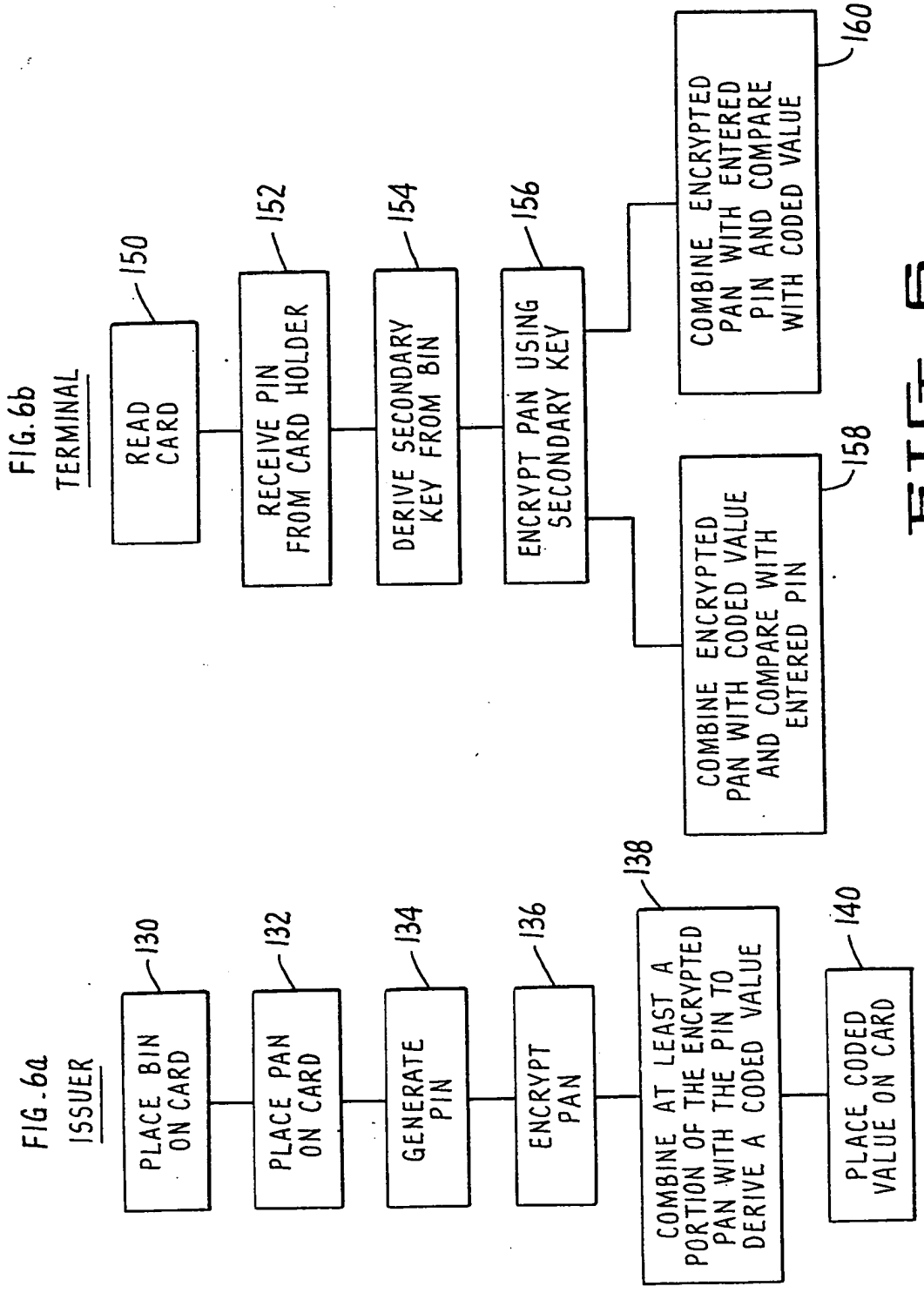


FIG. 6.

0138320

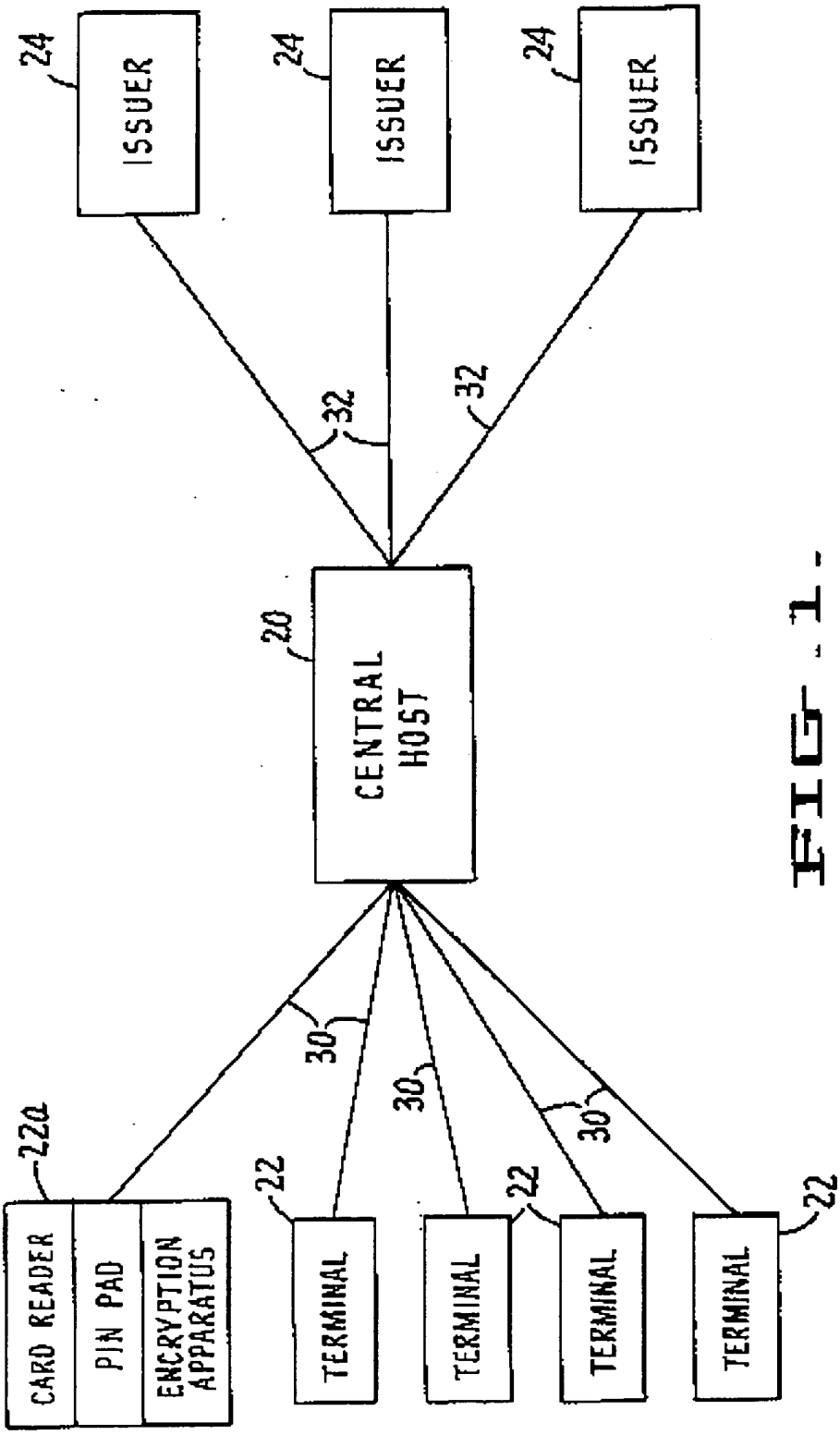


FIG. 1.

0138320

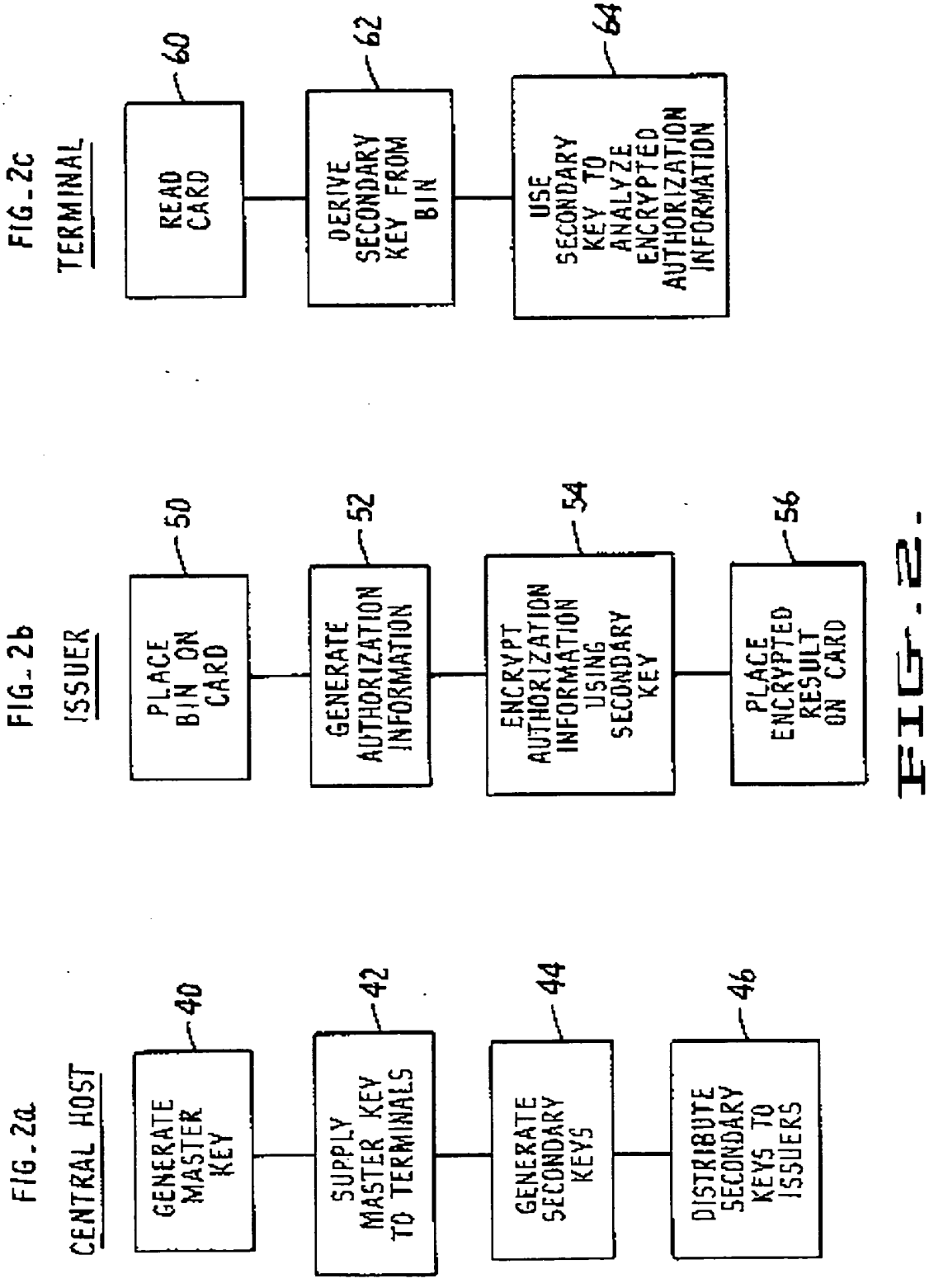


FIG. 2.

0138320

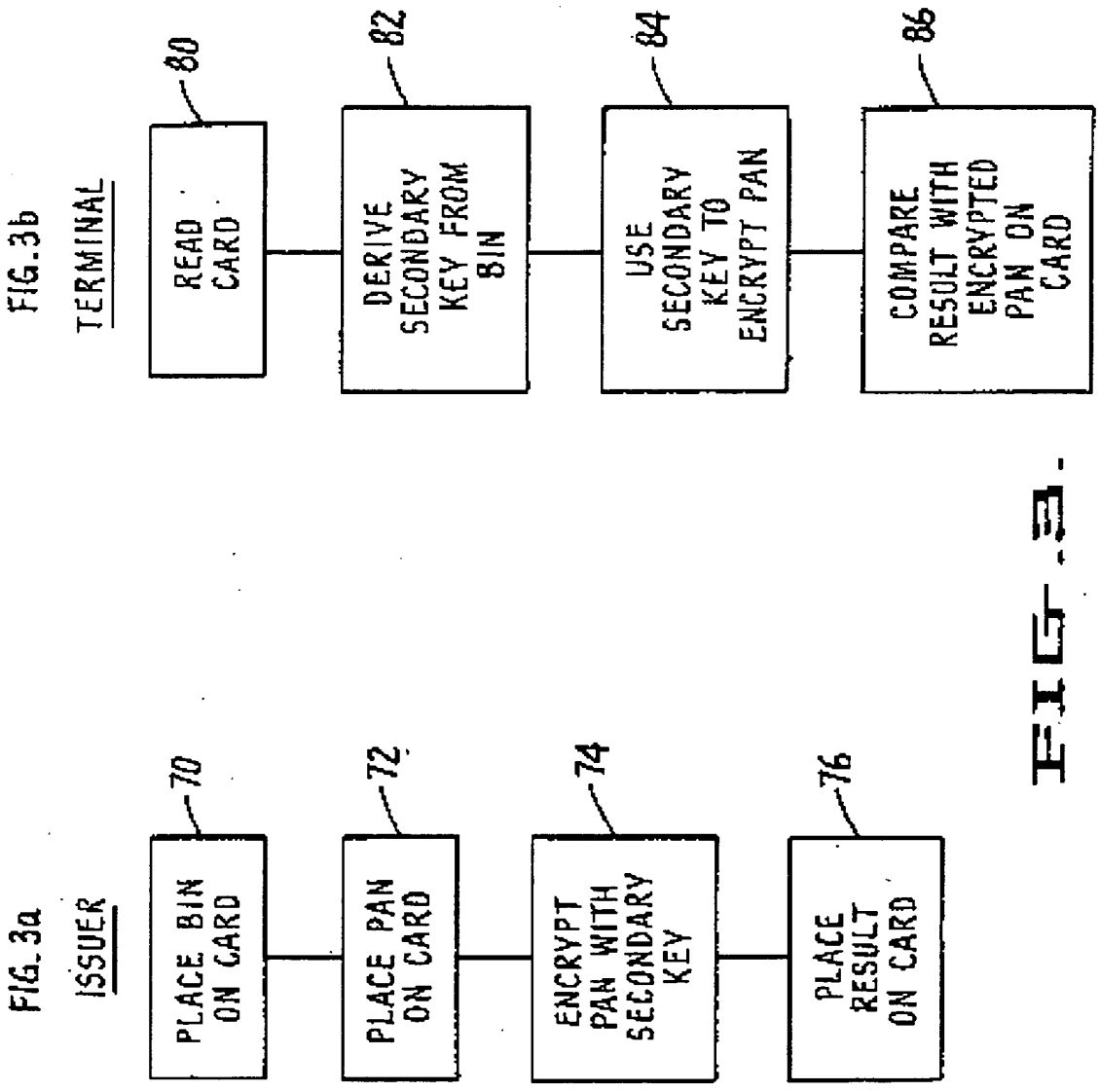


FIG.3.

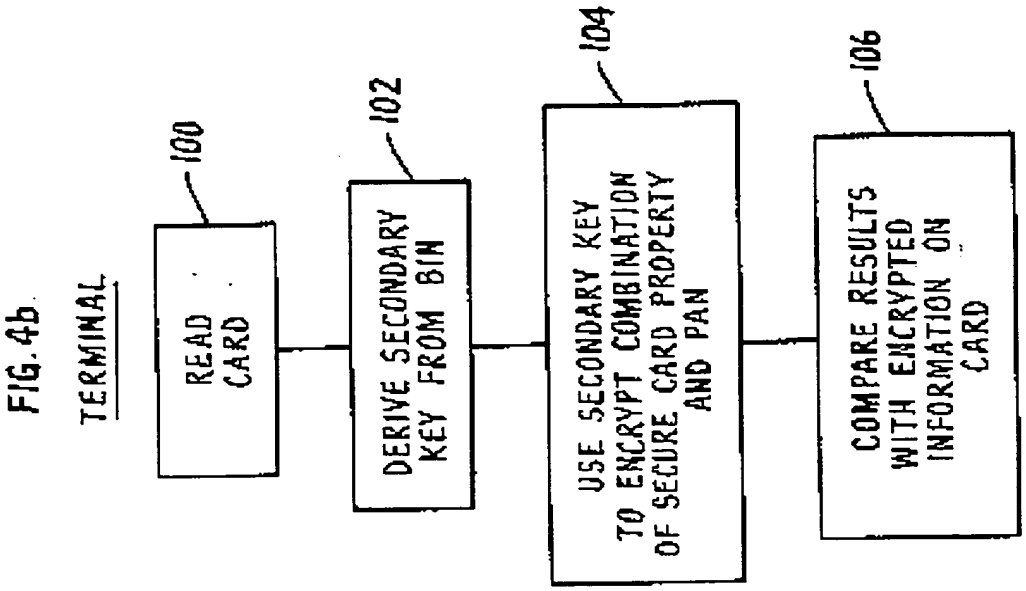
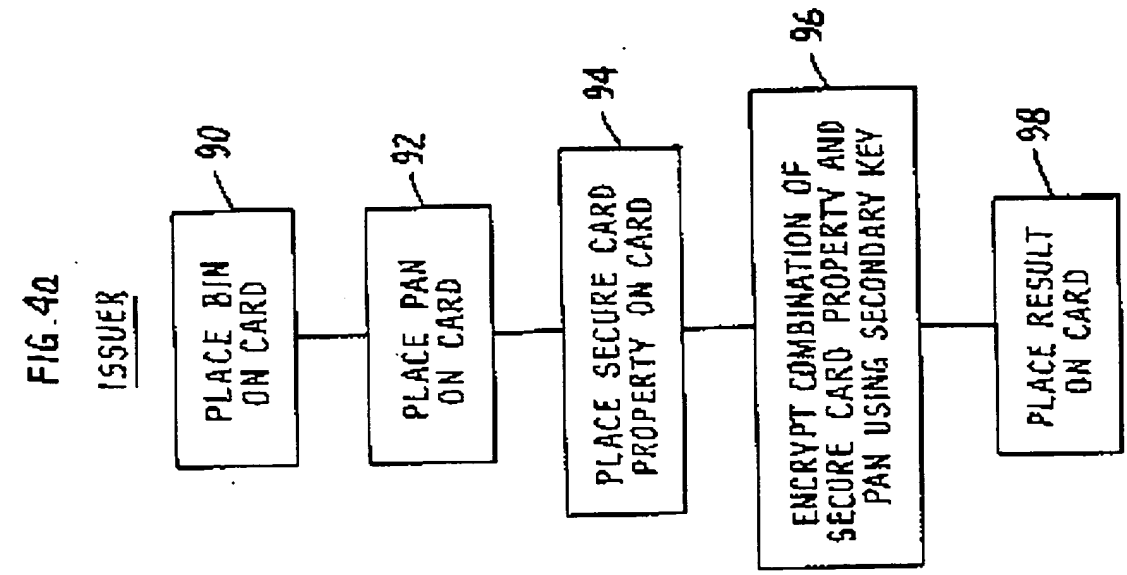


FIG. 4.



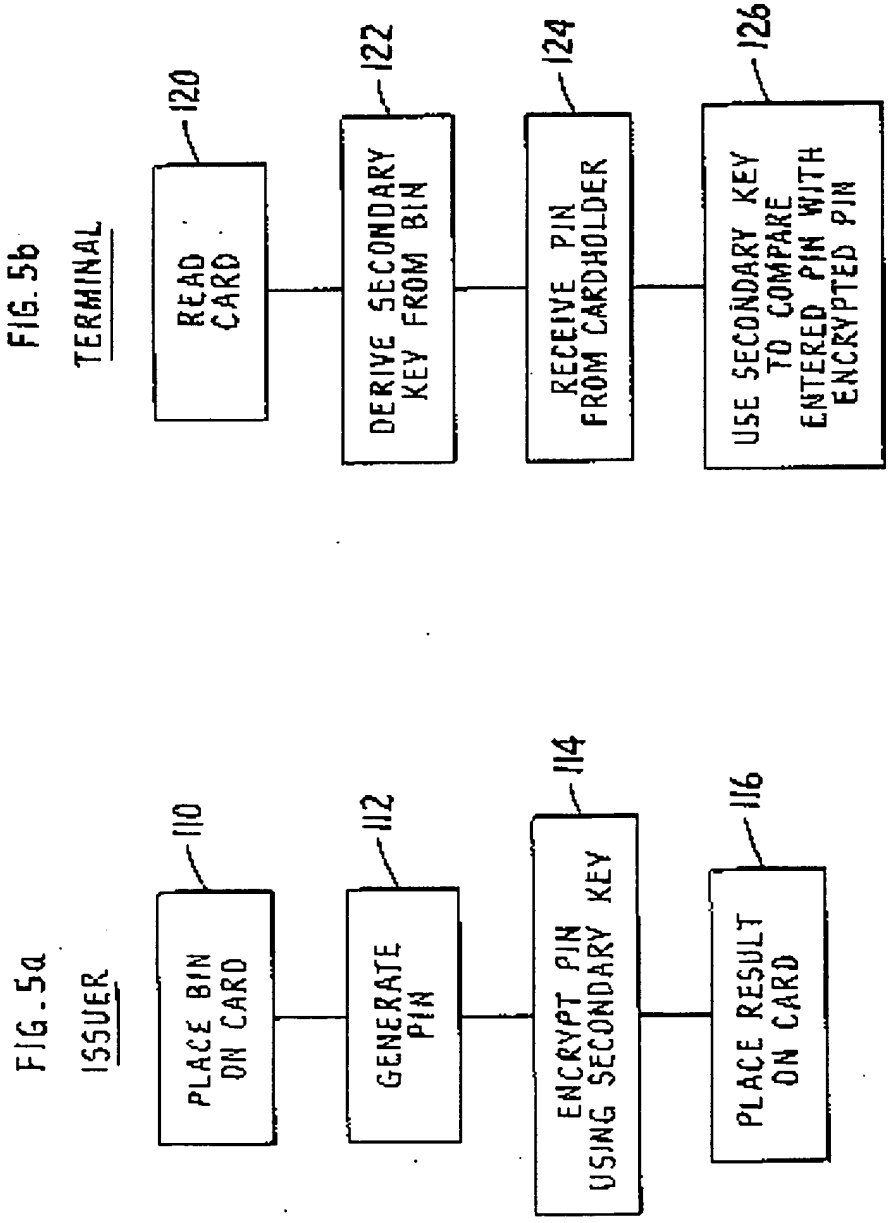


FIG. 5.

0138320

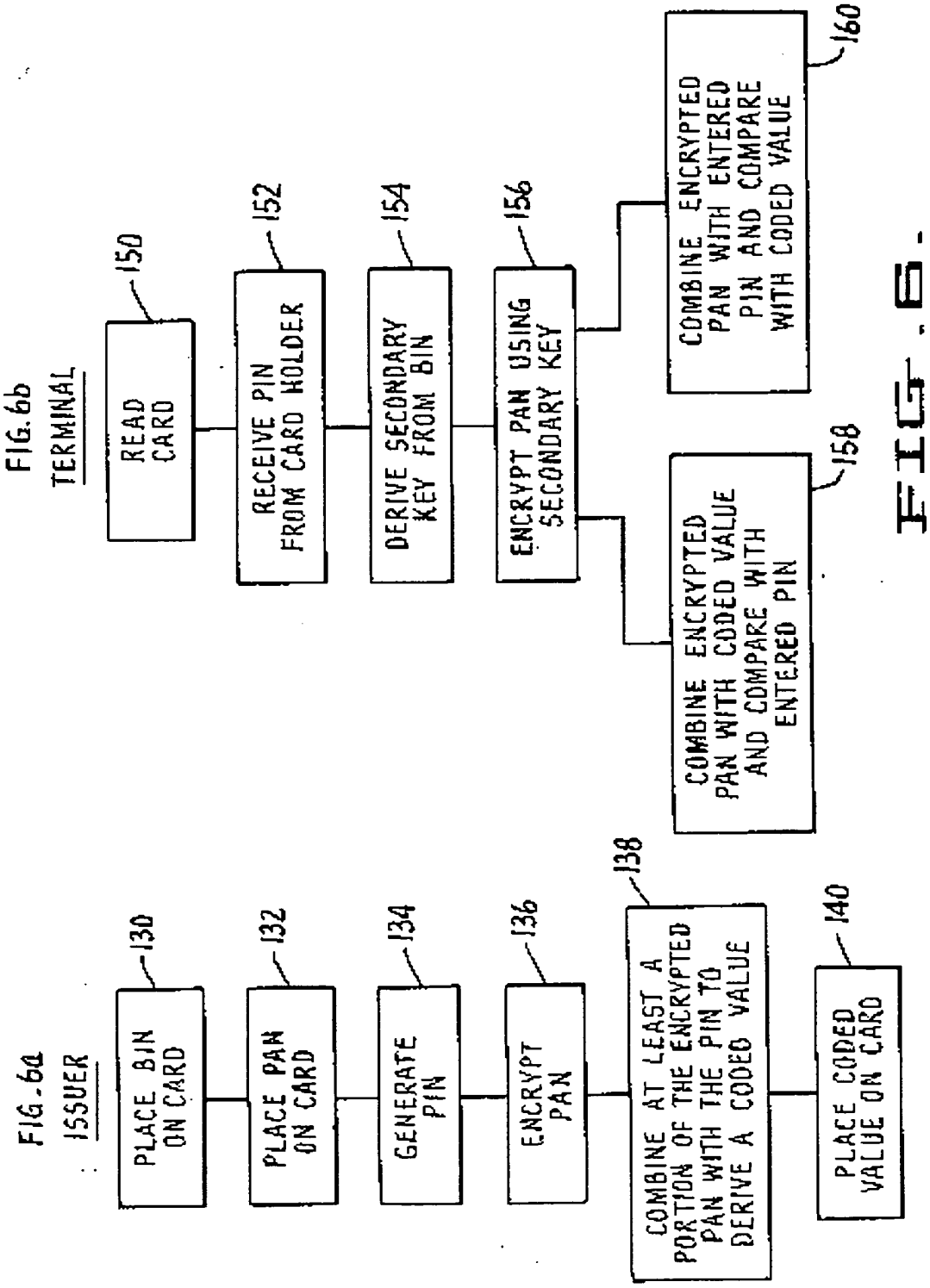


FIG. 6.